REMARKS

Claims 1-19, 21 and 22 are all the claims pending in the application.

I. Claim Rejections under 35 U.S.C. § 103(a)

A. Claims 1-7, 10-13, 15, 18, 19, 21 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Tagawa et al. (U.S. 7,096,504) in view of Otsuka et al. (U.S. 6,094,723).

Claim 1 recites the feature of a portable recording device that includes a "tamper-resistant module operable to judge, based on license information, whether an operation... is permitted, and when judged in the affirmative, to output to the information-processing device an instruction showing that the operation is permitted, and to rewrite the license information in accordance with the operation." Applicants respectfully submit that the combination of Tagawa and Otsuka does not teach or suggest such a feature.

Regarding Tagawa, Applicants note that this reference discloses a system in which a device is able to securely access copyrighted material stored on a SD memory card 100 by utilizing a usage rule stored in the SD memory card (see Abstract, col. 2, lines 3-7 and col. 7, lines 60-61). In this regard, in Tagawa, several examples are disclosed pertaining to the ability of a connected device to obtain the copyrighted material stored in the SD memory card 100 (see col. 9, lines 1-4). The examples shown in Fig. 4C and 4D, which were relied on by the Examiner in the Office Action, are described below.

In the example shown in Fig. 4C, the usage rule stored in the SD memory card 100 indicates that one move of the copyrighted material is permitted, which means that the connected device can read the copyrighted material from the SD memory card 100 and store in on an internalized medium (see col. 9, lines 28-33). As explained in Tagawa, when the usage rule is recorded on the internalized medium of the connected device, the copyrighted material as well as the usage rights exists on both of the internal recording medium of the connected device and on the SD memory card 100, and therefore, the connected device performs processing to delete the copyrighted material from the SD memory card 100 (see col. 9, lines 33-41).

In the example shown in Fig. 4D, the usage rule stored in the SD memory card 100 indicates that no moves of the copyrighted material are permitted, and thus, the usage rule cannot

be moved and the connected device cannot obtain management rights (see col. 9, lines 45-48). As explained in Tagawa, when the permitted number of moves is zero, this indicates that the permitted number of moves was originally one or more, but that the copyrighted material has been moved to a device one or more times, and the number of permitted moves was decremented until reaching zero (see col. 9, lines 48-54).

In Tagawa, regarding the actual transfer of the copyrighted material from the SD memory card 100 to the connected device, Applicants note that Tagawa describes that if a request is received to move copyrighted material from the SD memory card 100 to a local storage device 32 of the connected device, that a library control unit 37 of the connected device reads the usage rule from the SD memory card 100 in order to determine whether the copyrighted material can be transferred from the SD memory card 100 to the connected device (see Fig. 34A and col. 28, lines 53-57).

In this regard, as explained in Tagawa, if the library control unit 37 (which is part of the connected device) determines that the number of permitted moves is zero, then moving the copyrighted material from the SD memory card 100 to the local storage 32 of the connected device is prohibited (see col. 28, line 66 through col. 29, line 2). On the other hand, if the library control unit 37 determines that the number of permitted moves is one or more, then the library control unit 37 decrements the number of permitted moves, and performs a secure write of the usage rule and the copyrighted material from the SD memory card 100 to the local storage 32 of the connected device (see col. 29, lines 4-17 and lines 35-41).

Therefore, in summary, Applicants note that in Tagawa, if the connected device determines that the usage rule stored in the SD memory card 100 is one or more, then the connected device operates so as to decrement the number of moves of the usage rule (e.g., from 1 to 0), and to perform a secure write of the usage rule and the copyrighted material from the SD memory card 100 to the local storage 32 of the connected device (e.g., see col. 29, lines 4-17 and lines 35-41).

As noted above, claim 1 recites that the portable recording device includes a tamper-resistant module that is operable to judge, based on license information, ... whether an operation ... is permitted, and when judged in the affirmative, to output to the information-processing

device an instruction showing that the operation is permitted, and to rewrite the license information in accordance with the operation.

Thus, according to claim 1, it is the portable recording device which judges whether the operation is permitted based on the license information, which outputs to the information-processing device an instruction showing that the operation is permitted, and which rewrites the license information.

In direct contrast, as described above, in Tagawa, it is the connected device (i.e., not the SD memory card 100) which determines whether the copyrighted material can be moved from the SD memory card to the connected device, and which rewrites the usage rule stored in the SD memory card by decrementing the number of moves of the usage rule.

In view of the foregoing, Applicants respectfully submit that Tagawa does not disclose, suggest or otherwise render obvious at least the above-noted feature recited in claim 1 of a portable recording device that includes a tamper-resistant module operable to judge, based on license information, whether an operation... is permitted, and when judged in the affirmative, to output to the information-processing device an instruction showing that the operation is permitted, and to rewrite the license information in accordance with the operation. Further, Applicants respectfully submit that Otsuka fails to cure this deficiency of Tagawa.

Accordingly, Applicants submit that claim 1 is patentable over the cited prior art, an indication of which is kindly requested. Claims 2-4 depend from claim 1 and are therefore considered patentable at least by virtue of their dependency.

Moreover, regarding claim 1, Applicants note that in the Office Action, the Examiner indicated that "the information processing device is actually managed by the memory card security module because if the connected device (i.e., the information processing device cannot obtain usage information/rule from the memory card, then the information processing device has no way to make any determination by itself whether the permission should be granted or not..." (see Office Action at page 3).

In response to the above-noted comment by the Examiner, Applicants note that the Examiner has evidently misunderstood the disclosure in Tagawa. As described above, in Tagawa, it is clearly disclosed that the library control unit 37 of the connected device is able to

access the usage rule of the SD memory card 100 and determine the number of permitted moves, even if the number of permitted moves is zero (see Fig. 34A and col. 28, line 53 through col. 29, line 5).

With respect to the disclosure in Tagawa at col. 9, lines 45-48 which indicates that when the usage rule shows zero permitted moves, that the usage rule cannot be moved and the connected device cannot obtain "management rights", Applicants note that this disclosure does not mean that the connected device cannot access the usage rule and determine that the usage rule shows zero permitted moves. Instead, it simply means that when the connected device determines that the usage rule shows zero permitted moves, that the connected device is not able to move the usage rule from the SD memory card 100, and that because the copyrighted material cannot be transferred to the connected device, that the connected device will not have "management rights" to the copyrighted material.

Again, as explained above, Tagawa explicitly discloses that the connected device can access the SD memory card 100 so as to determine the usage rule, regardless of the number of permitted moves that are indicated by the usage rule (see Fig. 34A and col. 28, line 53 through col. 29, line 5).

Furthermore, with respect to claim 1, Applicants note that the Examiner has also indicated in the Office Action that the "permission instruction is obviously equivalent to be determined solely from the security module (e.g., AKE -- authentication processing unit) on the memory card - i.e., the permission is granted only when the connected device has successfully performed AKE processing" (see Office Action at pages 3-4).

In response to the above-noted comment by the Examiner, Applicants note that the Examiner has evidently misunderstood the disclosure in Tagawa. In particular, Applicants note that the Examiner appears to believe that if the AKE processing is successful in Tagawa, that the SD memory card 100 will judge that the copyrighted material can be accessed by the connected device. Regarding such a position, Applicants respectfully point out to the Examiner that the AKE processing in Tagawa has absolutely nothing to do with the determination based on the usage rule as to whether the copyrighted material can be accessed by the connected device.

For example, with respect to the AKE processing units 4 and 5 of Tagawa, Applicants

note that these units perform mutual authentication between a connected device and the SD memory card 100 using a challenge-response method in order to determine whether the connected device is valid (see col. 7, line 62 through col. 8, line 2). The determination as to whether the connected device is valid, however, does not determine whether or not the copyrighted material stored in the SD memory card 100 can be accessed by the connected device. Instead, it is the usage rule stored in the SD memory card which effects whether the copyrighted material can be accessed by the connected device. Specifically, the connected device determines whether the copyrighted material can be accessed based on the number of permitted moves of the usage rule, as described above.

As a further illustration, suppose that a specific piece of copyrighted material stored on the SD memory card of Tagawa had a corresponding usage rule which indicated that there is only one permitted move. In such a situation, if a connected device attempts to read the copyrighted material for a second time, even though the mutual authentication using the AKE units may be successful (i.e., the connected device is a valid device), due to the usage rule, the connected device will not be able to read the copyrighted material from the SD memory card 100.

Based on the foregoing, Applicants respectfully submit that claim 1 is patentable over the cited prior art, an indication of which is kindly requested.

Claim 5 recites the feature of a tamper-resistant module operable to judge, based on the license information, whether an operation, being one of installing software on an information-processing device and deactivating installed software, is permitted, and when judged in the affirmative, to output to the information-processing device an instruction showing that the operation is permitted, and to rewrite the license information in accordance with the operation.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that the combination of Tagawa and Otsuka does not teach, suggest or otherwise render obvious such a feature. Accordingly, Applicants submit that claim 5 is patentable over the cited prior art, an indication of which is kindly requested. Claims 6, 7 and 10-13 depend from claim 5 and are therefore considered patentable at least by virtue of their dependency.

Regarding claim 15, Applicants note that this claim is drawn to an information-

processing device that performs at least one of installing and deactivating software, the information-processing device comprising: a receiving unit operable to receive an instruction from a portable recording device; and a control unit operable to perform, in accordance with the received instruction, one of (i) receiving software from the portable recording device and installing the received software in said information-processing device, and (ii) deactivating installed software, wherein the portable recording device includes a tamper-resistant module operable to judge, based on the license information, whether an operation, being one of installing software on said information-processing device and deactivating installed software, is permitted, and when judged in the affirmative, to output to said information-processing device an instruction showing that the operation is permitted, and to rewrite the license information in accordance with the operation.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that the combination of Tagawa and Otsuka does not teach, suggest or otherwise render obvious such features. Accordingly, Applicants submit that claim 15 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claim 18, Applicants note that this claim is drawn to a control method used by a portable recording device that includes a normal storage unit having stored therein software that is computer data, a secure storage unit not directly accessible from outside and having stored therein license information relating to a usage condition of the software, and a tamper-resistant module, the control method comprising judging, based on the license information, whether an operation, being one of installing software on an information-processing device and deactivating installed software, is permitted; outputting to the information-processing device when judged in the affirmative, an instruction showing the operation to be permitted; and rewriting the license information in accordance with the operation.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that the combination of Tagawa and Otsuka does not teach, suggest or otherwise render obvious such features. Accordingly, Applicants submit that claim 18 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claim 19, Applicants note that this claim recites the feature of judging, based

on the license information stored in the secure storage unit, whether an operation, being one of installing software on an information-processing device and deactivating installed software, is permitted; outputting to the information-processing device when judged in the affirmative, an instruction showing the operation to be permitted; and rewriting the license information in accordance with the operation.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that the combination of Tagawa and Otsuka does not teach, suggest or otherwise render obvious such features. Accordingly, Applicants submit that claim 19 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claims 21 and 22, Applicants note that each of these claims recites the features of receiving an instruction from a portable recording device; and performing, in accordance with the received instruction, one of (i) receiving software from the portable recording device and installing the received software in the information-processing device, and (ii) deactivating installed software, wherein the portable recording device includes a tamper-resistant module operable to judge, based on the license information, whether an operation, being one of installing software on the information-processing device and deactivating installed software, is permitted, and when judged in the affirmative, to output to the information-processing device an instruction showing that the operation is permitted, and to rewrite the license information in accordance with the operation.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that the combination of Tagawa and Otsuka does not teach, suggest or otherwise render obvious such features. Accordingly, Applicants submit that claims 21 and 22 are patentable over the cited prior art, an indication of which is kindly requested.

B. Claims 8, 9, 16 and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Tagawa et al. (U.S. 7,096,504) in view of Otsuka et al. (U.S. 6,094,723), and further in view of Talstra et al. (U.S. 2005/0076225).

Regarding claims 8 and 16, Applicants note that claim 8 depends from claim 5, and that claim 16 depends from claim 15. Applicants respectfully submit that Talstra does not cure the

deficiencies of Tagawa and Otsuka, as discussed above, with respect to claims 5 and 15. Accordingly, Applicants submit that claims 8 and 16 are patentable at least by virtue of their dependency.

Regarding claim 9, Applicants note that this claim is drawn to a recording medium comprising a tamper-resistant module operable to judge, based on the license information, whether an operation, being one of installing software on an information-processing device and deactivating installed software, is permitted, and when judged in the affirmative, to extract the signature data from the license information, to output the extracted signature data to the information-processing device, and to rewrite the license information in accordance with the operation.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that the combination of Tagawa and Otsuka does not teach, suggest or otherwise render obvious such features. Further, Applicants respectfully submit that Talstra does not cure the deficiencies of Tagawa and Otsuka. In view of the foregoing, Applicants respectfully submit that claim 9 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claim 17, Applicants note that this claim is drawn to an information-processing device comprising a receiving unit operable to receive an instruction from a recording medium; and a control unit operable to perform, in accordance with the received instruction, one of (i) receiving software from the recording medium and installing the received software in said information-processing device, and (ii) deactivating installed software, wherein the recording medium includes a tamper-resistant module operable to judge, based on the license information, whether an operation is permitted, and when judged in the affirmative, to extract the signature data from the license information, to output the extracted signature data to said information-processing device, and to rewrite the license information in accordance with the operation.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Tagawa and Otsuka do not disclose, suggest or otherwise render obvious such features. Further, Applicants respectfully submit that Talstra does not cure the deficiencies of Tagawa and Otsuka. Accordingly, Applicants respectfully submit that claim 17 is patentable

over the cited prior art, an indication of which is kindly requested.

C. Claim 14 was rejected under 35 U.S.C. §103(a) as being unpatentable over Tagawa et al. (U.S. 7,096,504) in view of Otsuka et al. (U.S. 6,094,723), and further in view of Jones et al. (U.S. 2002/0111996).

Claim 14 depends from claim 5. Applicants respectfully submit that Jones does not cure the deficiencies of Tagawa and Otsuka, as discussed above, with respect to claim 5. Accordingly, Applicants submit that claim 14 is patentable at least by virtue of its dependency.

II. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Shunji HARADA et al.

By: _____
Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/ra
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
January 11, 2008